REMARKS/ARGUMENTS

Favorable reconsideration of this application is respectfully requested.

Claims 21 and 22 are present in this application and stand rejected under 35 U.S.C. § 112, second paragraph, and under 35 U.S.C. § 102(e) over U.S. 7,178,137 (Shimada et al.).

Regarding the 35 U.S.C. § 112 rejection, claim 21 is amended to positively recite generating the first, second and third keys, and claim 22 is amended to positively recite generating the new first key. The claims are believed to complete and recite the generating or obtaining of each of the keys recited in the recording apparatus of claims 21 and 22. Withdrawal of the § 112 rejection is respectfully requested.

The Office Action also explains a few interpretations of claims 21 and 22 made with regard to the 35 U.S.C. § 112 rejection. On page 3 it is interpreted "that the claimed invention intends to limit the amount of information that is transferred when moving contents from the first recording medium to a second recording medium." The Applicants respectfully submit that such an interpretation is unduly limiting, and it is more instructive to consider Claim 21 to be directed to an apparatus having the feature that after content is copied from a first recording medium to a second recording medium, the function of the first recording medium is reduced from reproduction and copying of content to only reproduction of content, and the function of reproducing and moving the content is imparted to the second recording medium. Claim 22 includes the feature that after the content is moved from the second recording medium to a third recording medium, the reproduction/movement function of the second recording medium is disabled, and the function of reproducing and moving the content is shifted to the third recording medium.

Regarding the medium, move and third keys, the examiner is correct that these keys are generated in the encryption section and not in the processing section. Applicants also note that the processing section obtains the contents by decoding the first encrypted contents

from the encryption section using the first key. In the process of moving the contents from the first recording medium to the second recording medium, the processing section obtains the contents from the first recording medium by decoding the first encrypted contents using the first key.

The Applicants believe that examination of this application will be substantially enhanced by a thorough explanation of the operation of the claimed apparatus. The claimed apparatus performs a complex technique of moving content using a recorder as shown in Figure B attached to this response. Suppose that content A is recorded on a medium α along with a medium key (Enc-TK) and a move key (Move-Key). At this point in time, content A can be reproduced and copied from medium α.

After content A on medium α is recorded onto medium β along with the move key (Move-Key) it can be reproduced on and moved from medium β. At this time, on medium α only content A and the medium key (Enc-TK) are left, and hence only reproduction of content A is possible. Referring again to Figure B, after content A on medium β is recorded onto medium γ along with the move key (Move-key), it can be reproduced on and moved from medium γ. At this time, on medium β reproduction of content A is no longer possible. After content A on medium γ is recorded onto medium δ along with the move key (Move-key), it can be reproduced on and moved from medium δ. At this time, on medium γ, reproduction of content A is impossible.

Figure B illustrates the states of the content and the keys for the various mediums α-δ, and the presence of the appropriate keys will allow appropriate reproduction and moving of data, and the lack of keys will prevent reproduction and/or moving of the data. Content is moved between recording mediums along with the medium key (Enc-TK) and move key (Move-key) using a recorder. As a result of the movements, the medium key (Enc-TK) and move key (Move-Key) are left on only two of the mediums, and therefore one medium on

which the content can be reproduced and one medium from which content can be moved are left.

More specifically, the Applicants have prepared the attached annotated claims (Appendix 1) and the attached table (Appendix 2) to further assist in the understanding of the present invention. The annotated claims and table represent a non-limiting example provided for understanding the invention, is not meant to limit the invention. Referring to Figures 1, 9 and 10, the example proceeds using mediums D1, D2 and D3. A recording apparatus includes driver V1 and encoder M1. Contents are encrypted in the encryption section using a first key TK and a key DvK1 specific to the encoder is processed using medium key block information MKB read from the first recording medium D1. The process key is processed using medium-specific information (M-ID) read from D1 thereby generating second key MUK. The first key is encrypted using MUK to generate a medium key (Enc-TK), and the medium key is multiply encrypted using the third key MM to generate a move key (Enc2-TK). A key DvK2 specific to the driver is processed using the medium key block information to generate a fourth key MMK. The third key is encrypted using the fourth key MMK.

When recording content onto D1, the processing section records first encrypted contents (Enc-Contents) encrypted using the first key, Enc-TK and move key Enc2-TK which are supplied from the encryption section. A third key Enc-MM is encrypted using the forth key onto a security area on the first recording medium.

When moving contents from D1 to D2, the first key is obtained by decoding the medium key using the second key (see step S25) and the contents are obtained by decoding the first encrypted contents using the first key. The contents are encrypted into new encrypted contents (Enc-Contents) using a new first key TK2 (see also step S25). Key DvK1 specific to the encoder is processed using the new medium key block information MKB2 read

from D2. The process key is processed using new medium specific key (M-ID2) read from D2, thereby generating new second key MUK2 (see step S27). The new first key is multiply encrypted using the new second key and the new third key to generate a new move key (Enc2-TK2), as shown in step S28, and key DvK2 is processed using MKB2, thereby generating a new fourth key MMK2. On D2, new encrypted contents are recorded encrypted using the new first key, and the new move key is recorded. On a security area on D2, the new third key encrypted using the new fourth key is recorded, as shown in steps S28 and S29. The move key is erased from the first medium, as shown in step S26.

The apparatus of Claim 21 enables the same key information (MK) to be produced even from a plurality of device keys (DvK) thereby realizing replay, and other replay apparatuses, of contents recorded onto a certain optical disk and also to enable certain mediums to be bound by medium specific information (M-ID), thereby preventing the entire data from being copied to other mediums.

The apparatus also provides for an improved method of moving contents. Two keys are employed, i.e., the medium key (Enc-TK) for versatile replay devices and a move key (Move-Key) for contents movement. When contents are recorded onto a first disk, D1, two keys are also recorded thereon to enable the contents to be further moved to another disk and to be replayed even by a versatile device other than by a dedicated device. When the contents are further moved from D1 to a second disk D2, the move key is erased from the first disk D1 and only the medium key (Enc-TK) for enabling the contents to be replayed by versatile devices is left on D1. Further movement of contents on D1 is disabled while D1 can still be replayed. When contents are moved to D2, only the move key is recorded onto D2. Hence, the second disk can be replayed only by the dedicated device, and further movement of the contents to a third disk is enabled.

In the apparatus of claim 22, the Applicants refer the Examiner to the non-limiting examples of Figures 5 and 11 where movement of contents from D2 to a third disk D3 is described. The new move key (Enc2-TK2) is decoded using the new second key (MUK2) and the new third key (MM2), thereby obtaining the first key, as described in steps S31 and S43. The new encrypted contents are decoded using the new first key to obtain the contents, and the contents are encrypted using a renewed first key (TK3) thereby obtaining renewed contents (Enc-Contents), as described in step S43. Key DvK1 is processed using renewed medium key block information MKB3 read from D3 and the processed key is processed using renewed specific information M-ID3 read from D3, to obtain a renewed second key MUK3, as described in step S27.

The renewed first key is multiply encrypted using the renewed second key and the renewed third key, thereby producing a renewed move key (Enc2-TK3), as described in step S28. Key DvK2 specific to the driver is processed using the renewed medium key block information MKB3, thereby producing a renewed fourth key MMK3, as described in step S28. The renewed encrypted contents are recorded onto D3 using the renewed first key, and the renewed move key is recorded on D3, as shown in step S29. The renewed third key Enc-MM3 is encrypted using the renewed fourth key and recorded onto a security area of D3. The new move key is erased from the second recording medium.

In the apparatus of Claim 22, the move key can be erased from D2 after it is moved to D3, whereby movement and replay of the contents on the second recording medium are inhibited. On the other hand D3 records only the move key, which means that replay and further movement of the contents are possible only when the dedicated device that employs contents management of the invention is used.

Turning to the § 102 rejection, Shimada merely discloses a system where content is supplied to a plurality of client terminals via the internet, as shown in attached reference

Figure A. At this time, ID data or content key is used to prevent illegal copying. Shimada clearly discloses an apparatus very different from the apparatus of claims 21-22. The Office Action further only generally points to Shimada without identifying the specific operations and elements recited in claims 21 and 22. For example, none of the keys or recited in the claims are specifically identified. It is respectfully submitted that it is clear that Shimada does not disclose a recording apparatus using the keys recited in claims 21-22.

Shimada discloses encrypting content with a Content-Key, and forming an MC-Key used to decrypt the User-ID, MID, Content-Key and Content-Gen-Key. The Content-Gen-Key is used to re-encrypt content for copying to HDD 2 (see columns 8-10). Neither of the Content-Key or Content-Gen-Key is encrypted with anything that would correspond to the recited second key. Further, there is no key that is multiply encrypted using another key to generate yet another key that corresponds to the recited move key or recited new move key. Nothing in Shimada corresponds to the recited move key is recorded onto a second recording medium. No move key is erase in Shimada. It is clearly not possible to reject claims 21-22 using Shimada and the rejection must be withdrawn

The Applicants respectfully request an interview so that the clear differences between Shimada and claims 21-22 can be explained, and the Examiner can identify every element of claims 21-22 in Shimada so that the basis for rejecting these claims can be understood.

The Examiner is respectfully requested to identify every element in claims 21-22 in any reference used to reject the pending claims.

It is respectfully submitted that the present application is in condition for allowance, and a favorable decision to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Registration No. 28,870

Carl E. Schlier
Registration No. 34,426
Attorneys of Record

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

APPENDIX 1

Claim 21. A recording apparatus including a driver (V1) and an encoder (M1), comprising:

an encrypting section which performs the following:

generating a first key (TK) by means of a first random number generator;

encrypting contents into first encrypted contents using the first key (TK);

processing a key (DvK1) specific to the encoder using medium key block information (MKB) read from a first recording medium (D1), processing the processed key using medium specific information (M-ID) read from the first recording medium (D1), thereby generating a second key (MUK);

encrypting the first key (TK) using the second key (MUK), thereby generating a medium key (Enc-TK);

generating a third key (MM) by means of a second random number generator;

multiple-encrypting the medium key (Enc-TK) using the third key (MM), thereby generating a move key (Enc2-TK);

processing a key (DvK2) specific to the driver using the medium key block information (MKB), thereby generating a fourth key (MMK); and

encrypting the third key using the fourth key (MMK); and

a processing section which performs the following when recording the contents onto the first recording medium (D1):

recording, onto the first recording medium (D1), first encrypted contents (Enc-Contents) the medium key (Enc-TK) and the move key (Enc2-TK), which are supplied from the encrypting section (step S16); and

recording the third key (Enc-MM) encrypted using the fourth key onto a secret area on the first recording medium (steps S17 and S18),

wherein the processing section which performs the following when moving the contents from the first recording medium (D1) to a second recording medium (D2):

obtaining the second key (MUK) generated in the encrypting system;

obtaining the first key (TK) by decoding the medium key (Enc-TK) using the second key (step S25);

obtaining the contents by decoding the first encrypted contents using the first key,

generating a new first key (TK2) by means of the first random number generator;

encrypting the contents into new encrypted contents (Enc-Contents) using the new first key (TK2) (step S25):

processing the key (DvK1) specific to the encoder using new medium key block information (MKB2) read from the second recording medium (D2), and processing the processed key using new medium specific key (M-ID2) read from the second recording medium (D2), thereby generating a new second key (MUK2) (step S27);

generating a new third key (MM2) by means of the second random number generator;

multiply-encrypting the new first key using the new second key and the new third key, thereby generating a new move key (Enc2-TK2) (step S28);

processing the key (DvK2) specific to the driver using the new key specific block information (MKB2), thereby generating a new fourth key (MMK2);

recording, onto the second recording medium (D2), the new move key (Enc-TK2) and encrypted contents (Enc-Contents) (step S29); and

recording, onto a security area on the second recording medium (D2), the new third key (Enc-MM2) encrypted using the new fourth key (steps S28 and S29); and

erasing the move key from the first medium (step S26).

Claim 22. The recording apparatus according to claim 1, wherein when the contents are moved from the second recording medium (D2) to a third recording medium (D3), the processing section performs the following:

generating a renewed first key (TK3);

decoding the new move key (Enc2-TK2) using the new second key (MUK2) and the new third key (MM2), thereby obtaining the first key (steps S31 and S43);

decoding the new encrypted contents using the new first key to obtain the contents, and encrypting the contents using the renewed first key (TK3), thereby obtaining renewed contents (Enc-Contents) (step S43);

processing the key (DvK1) specific to the encoder, using renewed medium key block information (MKB3) read from the third recording medium (D3), and processing the processed key using renewed specific information (M-1D3) read from the third recording medium (D3), thereby obtaining a renewed second key (MUK3) (step S27);

multiple-encrypting the renewed first key using the renewed second key (MUK3) and the renewed third key (MM3), thereby producing a renewed move key (Enc2-TK3) (step S28);

processing the key (DvK2) specific to the driver, using the renewed medium key block information (MKB3), thereby producing a renewed fourth key (MMK3) (step S28);

recording, onto the third recording medium (D3), renewed encrypted contents encrypted using the renewed first key, and the renewed move key (Enc2-TK3) (step S29);

recording, onto a security area on the third recording medium, the renewed third key (Enc-MM3) encrypted using the renewed fourth key (step S29); and

erasing the new move key from the second recording medium (step S26).

APPENDIX 2

Correspondence between mediums (D1, D2, D3), keys, information and contents

.

First Recording Medium (D1)	Second Recording Medium (D2)	Third recording medium (D3)
First key (TK)	New first key (TK2)	Renewed first key (TK3)
Second key (MUK)	New second key (MUK2)	Renewed second key (MUK3)
Third key (MM)	New third key (MM2)	Renewed third key (MM3)
Fourth key (MMK)	New fourth key (MMK2)	Renewed fourth key (MMK3)
Medium key (Enc-TK)	New medium key (Enc-TK2)	Renewed medium key (Enc-TK3)
Move key (Enc2-TK)	New move key (Enc2-TK2)	Renewed move key (Enc2-TK3)
Medium key block information (MKB)	New medium key block information (MKB2)	Renewed medium key block information (MKB3)
Medium specific information (M-ID)	New medium specific information (M-ID2)	Renewed medium specific information (M-ID3)
Encrypted contents (Enc-Contents)	New encrypted contents (Enc-Contents)	Renewed Encrypted contents (Enc-Contents)

FIG. A. Shimada

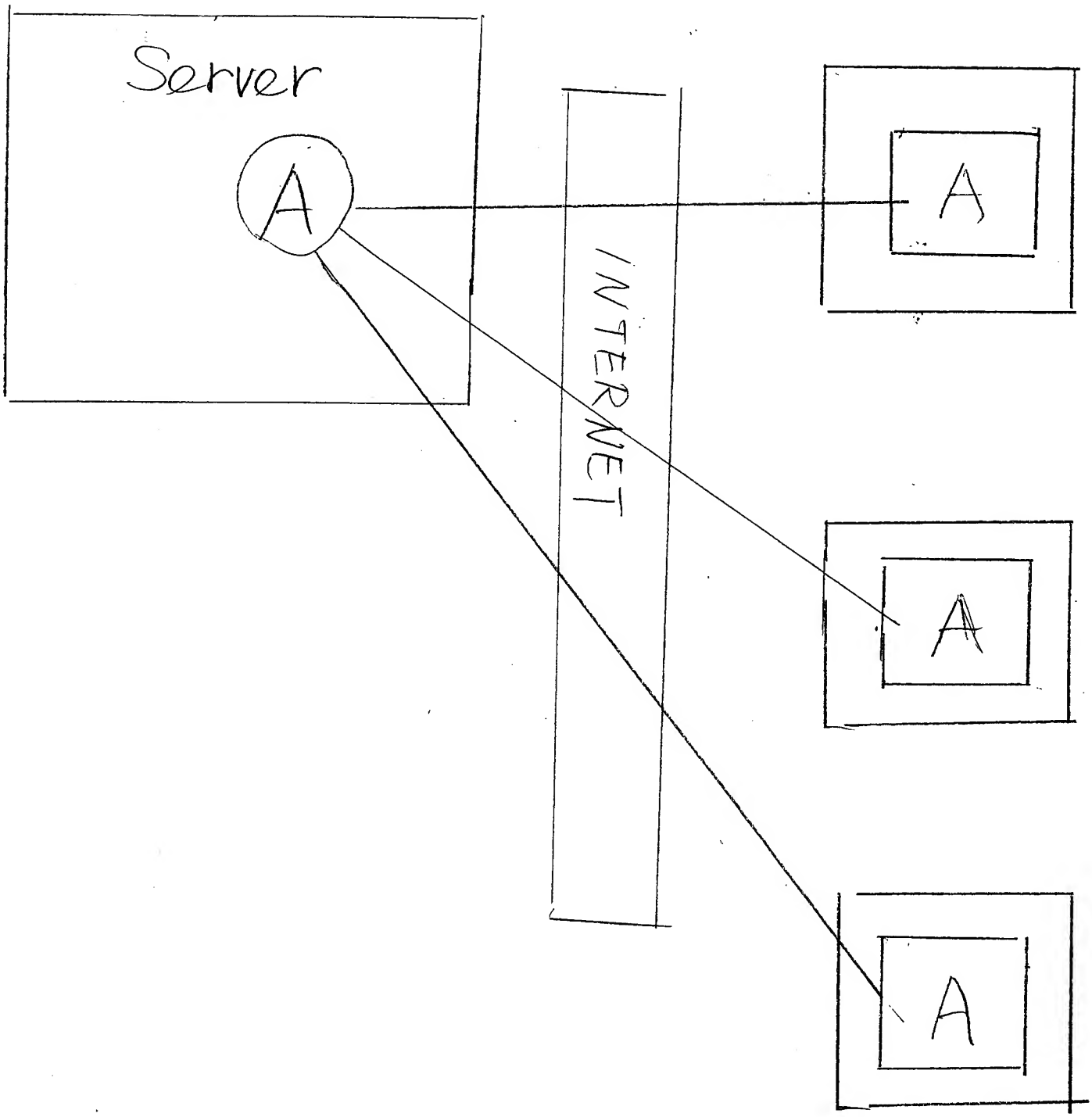

FIG. B Present Invention